



Homeland
Security

Daily Open Source Infrastructure Report

31 October 2014

Top Stories

- Superior Crude Gathering Inc., agreed October 29 to pay \$1.6 million in penalties to settle alleged violations of the Clean Water Act stemming from a 92,400 gallon crude oil spill from tanks at the company's oil storage facility in Ingleside, Texas, into an unnamed lake and wetlands in 2010. – *U.S. Environmental Protection Agency* (See item [1](#))
- Developers warned that Drupal Web sites that were not patched within 7 hours of the disclosure of a critical SQL injection vulnerability October 15 should be considered compromised and advised admins to restore their sites. – *The Register* (See item [24](#))
- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory warning about an ongoing attack campaign targeting human machine interface (HMI) products used in industrial control systems. – *Securityweek* (See item [28](#))
- The Chickamauga Lock was shut down and traffic on the Tennessee River stalled near Chattanooga, Tennessee, after the U.S. Army Corps of Engineers discovered an upper gate anchorage issue during a routine inspection October 27. – *WBIR 10 Knoxville* (See item [35](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *October 29, U.S. Environmental Protection Agency* – (Texas) **Texas company to pay \$1.6M for oil spill violations.** The U.S. Environmental Protection Agency and the U.S. Department of Justice reached a settlement with Texas-based Superior Crude Gathering Inc., (Superior Crude) October 29 for alleged violations of the Clean Water Act stemming from a 92,400 gallon crude oil spill from tanks at the company's oil storage facility in Ingleside into an unnamed lake and wetlands in 2010. Superior Crude will pay a \$1.6 million civil penalty.

Source:

<http://yosemite.epa.gov/OPA/ADMPRESS.NSF/d0cf6618525a9efb85257359003fb69d/0bcc7b168f89d77f85257d8000674455>

For another story, see item [28](#)

[\[Return to top\]](#)

Chemical Industry Sector

See item [28](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[\[Return to top\]](#)

Critical Manufacturing Sector

See item [28](#)

[\[Return to top\]](#)

Defense Industrial Base Sector

2. *October 29, U.S. Environmental Protection Agency* – (Louisiana) **EPA finalizes agreement for cleanup at Camp Minden.** The U.S. Environmental Protection Agency (EPA) finalized an agreement October 29 with the Louisiana Department of Environmental Quality (LDEQ), Louisiana Military Department (LMD), and the U.S. Army for the controlled burn disposal of more than 15 million pounds of smokeless propellants left abandoned at Camp Minden in Louisiana. The agreement becomes effective November 4 and the disposal of the explosives will be controlled by the LMD, with the EPA and LDEQ overseeing work and environmental safety at the site.

Source:

<http://yosemite.epa.gov/OPA/ADMPRESS.NSF/d0cf6618525a9efb85257359003fb69d/>

[\[Return to top\]](#)

Financial Services Sector

3. *October 29, Reuters* – (Illinois; Indiana) **Twenty-nine charged in Chicago with ‘cracking cards’ bank fraud scheme.** Prosecutors filed federal and State charges against 29 people in the Chicago area and in Hammond, Illinois, for allegedly running a bank fraud scheme that recruited individuals to hand over debit cards and then cash fraudulent checks to the accounts, causing bank losses of more than \$1.7 million. Source: <https://news.yahoo.com/twenty-nine-charged-chicago-cracking-cards-bank-fraud-181808332.html>
4. *October 29, IDG News Service* – (International) **Cybercriminals create platform for automating rogue credit card charges.** Researchers with IntelCrawler reported that a Web-based application known as Voxis Platform that automates purchases from stolen payment card data has been sold on underweb markets since August. The application purports to use 32 different payment gateways and other methods to mimic normal card use and avoid detection. Source: <http://www.networkworld.com/article/2840753/cybercriminals-create-platform-for-automating-rogue-credit-card-charges.html>

For another story, see item [33](#)

[\[Return to top\]](#)

Transportation Systems Sector

5. *October 29, KERO 23 Bakersfield* – (California) **Big rig wreck causes headaches on the Grapevine overnight.** Interstate 5 in Grapevine was closed for around 9 hours October 28 – October 29 when a semi-truck overturned and blocked all lanes, spilling produce and fuel and causing a small brush fire that burned several acres along the shoulder. Source: <http://www.turnto23.com/news/local-news/big-rig-wreck-causes-headaches-on-the-grapevine-overnight>
6. *October 29, Mid-Hudson News Network* – (New York) **Truck carrying deodorant chemicals overturns, shuts down Route 209.** Route 209 near Route 211 in the Town of Deerpark was closed for over 3 hours October 28 when a semi-truck carrying deodorant chemicals struck a utility pole after failing to negotiate a curve and overturned. Source: http://www.midhudsonnews.com/News/2014/October/29/Dpk_truck_acc-29Oct14.html
7. *October 29, Pasadena Star-News* – (California) **Big rig hits sign, rolls over on 210 Freeway in La Crescenta.** One person was injured when a semi-truck hit an overhead

sign and overturned on the eastbound 210 Freeway in La Crescenta October 28 and forced the closure of all eastbound lanes. All lanes were reopened October 29 after around 8 hours.

Source: <http://www.pasadenastarnews.com/general-news/20141029/big-rig-hits-sign-rolls-over-on-210-freeway-in-la-crescenta>

8. *October 29, San Antonio Express-News* – (Texas) **Crews working to clear 18-wheeler crash on I-10 near downtown.** Crews worked more than 12 hours overnight to clear the scene of an accident when a semi-truck traveling on the interchange from Interstate 35 to Interstate 10 West near San Antonio overturned and blocked 3 left lanes October 28. A second accident occurred when a vehicle hit a police vehicle that was part of the response to the initial accident, complicating cleanup.

Source: <http://www.mysanantonio.com/news/local/article/Crews-working-to-clear-18-wheeler-crash-on-I-10-5855230.php>

9. *October 27, Portsmouth Daily Times*– (Ohio) **Three injured in truck crash.** Ohio Route 73 at Noel Lane was closed for nearly 7 hours October 26 following a 3-vehicle crash that injured 3 people and caused a small amount of gasoline to be spilled onto the roadway.

Source: <http://portsmouth-dailytimes.com/news/news/150309658/Three-injured-in-truck-crash>

For additional stories, see items [15](#) and [35](#)

[\[Return to top\]](#)

Food and Agriculture Sector

10. *October 30, Associated Press* – (Iowa) **No injuries in eastern Iowa business fire.**

About 25 to 30 workers were evacuated from the Mills Manufacturing Company facility in Earlville October 29 after an oven used to produce agricultural powdered paint caught fire. Authorities are investigating the source of the fire which severely damaged the plant's equipment.

Source: <http://www.kwwl.com/story/27161668/no-injuries-in-eastern-iowa-business-fire>

11. *October 29, Food Safety News* – (Maryland; Alabama) **Virginia grower recalls one lot of fresh cilantro for potential Salmonella.** Shenandoah Growers Inc., of Harrisonburg, Virginia, announced October 29 a recall for 465 containers of its conventional fresh-cut cilantro due to possible Salmonella contamination. The products were packaged with Shenandoah Growers and Giant branding and were distributed to two customers in Maryland and Alabama.

Source: <http://www.foodsafetynews.com/2014/10/virginia-grower-recalls-one-lot-of-fresh-cilantro-for-potential-salmonella>

12. *October 29, Newton Daily News* – (Iowa) **DNR looks into manure spill in north-central Iowa.** The Iowa Department of Natural Resources is investigating after a

farmer in Hamilton County reported finding liquid manure pooled in his corn field due to an apparent leak from an underground manure pipeline October 27. Prestage Farms employees built a dike to prevent the manure from reaching waterways and are pumping manure into a nearby lagoon as they clean the scene.

Source: <http://www.newtondailynews.com/2014/10/29/dnr-looks-into-manure-spill-in-north-central-iowa/a9adtx1/>

13. *October 29, WPDE 15 Florence* – (South Carolina) **More than \$100,000 worth of farm equipment burned at a Dillon farm.** Six tractors, two combines, two grain trucks, and other planting equipment worth over \$100,000 was burned in an October 28-29 fire at a farm in Dillon. The cause of the fire is under investigation.

Source: <http://www.carolinalive.com/news/story.aspx?id=1116206>

14. *October 29, U.S. Department of Labor* – (Alabama) **Alabama's Wayne Farms poultry plant cited for exposing workers to musculoskeletal, other repeat, serious safety and health hazards.** The Occupational Safety and Health Administration October 29 cited Wayne Farms LLC, which makes Dutch Quality House and Platinum Harvest products, for 11 workplace safety and health violations at the company's Jack, Alabama poultry processing facility. Proposed penalties total \$102,600.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26922

For another story, see item [34](#)

[\[Return to top\]](#)

Water and Wastewater Systems Sector

15. *October 29, KOIN 6 Portland* – (Oregon) **HazMat called to Colton diesel spill.** Crews remained on-scene and worked to contain a spill October 29 after a semi-truck crashed on Highway 211 in Colton and spilled about 190 gallons of diesel fuel into a nearby creek October 28.

Source: <http://koin.com/2014/10/29/hazmat-called-to-colton-diesel-spill/>

16. *October 29, White Bear Lake Press* – (Minnesota) **Lost Lake sewer spill underestimated.** The Metropolitan Council's Environmental Services announced that it had underestimated the quantity of wastewater that spilled into Lost Lake October 4 and that based on new calculations an estimated total of 440,000 gallons of sewage spilled into the lake, up from the original 25,000 gallons reported.

Source: http://www.presspubs.com/white_bear/news/article_2d16be60-5ef9-11e4-9248-13b206848687.html

For another story, see item [28](#)

[\[Return to top\]](#)

Healthcare and Public Health Sector

Nothing to report

[\[Return to top\]](#)

Government Facilities Sector

17. *October 30, Winfield Daily Courier* – (Kansas) **Dexter Elementary School evacuated Wednesday morning.** At least 4 students were transported to area hospitals October 29 following a carbon monoxide leak at Dexter Elementary School in Kansas that prompted the evacuation of the school after a faulty heat exchange on a heating and air conditioning roof mount released the fumes. Crews will repair the damaged equipment. Source: http://www.winfieldcourier.com/news/article_c62b1f9e-5fec-11e4-a4b9-07829ec77abb.html
18. *October 29, Dark Reading* – (National) **White House says unclassified network hit in cyberattack.** A White House National Security Council official confirmed October 29 that an unclassified portion of the White House network was the victim of an ongoing cyberattack, resulting in temporary system outages and loss of network connectivity for some users. Authorities worked to mitigate the threat and the attack did not cause any damage to White House computers or systems. Source: <http://www.darkreading.com/attacks-breaches/white-house-says-unclassified-network-hit-in-cyberattack/d/d-id/1317060>
19. *October 29, Associated Press* – (California) **Military jet crashes in California, killing pilot.** Officials are investigating after the pilot of a military jet on a training exercise was killed when the jet crashed into an agricultural field as it was preparing to land at Naval Station Ventura County in Port Hueneme October 29. Source: <http://www.msn.com/en-us/news/us/military-jet-crashes-in-california-killing-pilot/ar-BBbYLq4>
20. *October 29, Harrisburg Patriot-News* – (Pennsylvania) **Bomb threat shuts down schools for second day.** A bomb threat made to a secondary school in the Adams County district prompted the closure of Fairfield Area School District schools October 29-30. Police searched the schools and deemed them safe before classes were scheduled to resume October 31. Source: http://www.pennlive.com/midstate/index.ssf/2014/10/fairfield_schools_closed_secon.html
21. *October 29, WBBM 2 Chicago* – (Illinois) **Harper High evacuated over carbon monoxide, up to 9 hospitalized.** Fire and police officials reported that Harper High School in Chicago was evacuated and closed October 29 due to elevated levels of carbon monoxide in the building which caused up to nine students and staff to be transported to area hospitals for symptoms. Source: <http://chicago.cbslocal.com/2014/10/29/high-carbon-monoxide-levels-found->

[at-south-side-school-4-hospitalized/](#)

[\[Return to top\]](#)

Emergency Services Sector

22. *October 29, KSPR 33 Springfield* – (Missouri) **Thousands in equipment stolen from fire department.** Officials are investigating after at least \$10,000 worth of equipment was discovered stolen from the Cedar Creek Fire Department in Springfield, Missouri, October 28.
Source: http://www.kspr.com/news/local/thousands-in-equipment-stolen-from-fire-department/21051620_29414440
23. *October 29, WTIU 30 Bloomington/WFIU 103.7 FM Bloomington* – (Indiana) **911 services in southern Indiana now working after outage.** Emergency 9-1-1 landline service was down for approximately 5 hours October 29 for more than 100,000 customers in several southern Indiana counties after an AT&T fiber line was cut.
Source: <http://indianapublicmedia.org/news/911-outage-southern-indiana-affecting-100000-residents-73951/>

For another story, see item [30](#)

[\[Return to top\]](#)

Information Technology Sector

24. *October 30, The Register* – (International) **Drupalocalypse! Devs say it's best to assume your CMS is owned.** The developers of the Drupal content management system (CMS) warned that Drupal Web sites that were not patched within 7 hours of the disclosure of a critical SQL injection vulnerability October 15 should be considered compromised due to the simplicity of the vulnerability and how quickly it was leveraged by attackers. The developers advised affected admins to restore their sites from backup since applying the patch would only close the vulnerability to future use, not remove any malware already in place.
Source: http://www.theregister.co.uk/2014/10/30/drupal_sites_considered_hosed_if_sql_i_hole_unclosed/
25. *October 30, Threatpost* – (International) **Popular Science website infected, serving malware.** Researchers from Websense Security Lab discovered and reported that the Web site of Popular Science magazine was compromised and injected with a malicious iFrame that redirects users to a site hosting the RIG Exploit Kit.
Source: <http://threatpost.com/popular-science-website-infected-serving-malware/109089>
26. *October 30, Securityweek* – (International) **“AirHopper” malware uses radio signals to steal data from isolated computers.** Researchers at the Ben Gurion University

created a proof-of-concept malware dubbed AirHopper that was used to demonstrate a data exfiltration attack against air gapped systems using radio signals produced by the target system's graphics card. The attack requires adding the malware to the target system and installing malicious code onto a nearby mobile device in order to set up the channel for transmitting the data sent from the target system.

Source: <http://www.securityweek.com/airhopper-malware-uses-radio-signals-steal-data-isolated-computers>

27. *October 29, Softpedia* – (International) **Gmail drafts used to exfiltrate data and send malicious instructions.** Shape Security researchers identified and reported a new variant of the IcoScript remote access trojan (RAT) that uses draft Gmail email messages to communicate with its operator and receive instructions in order to avoid detection. The researchers stated that the malware strain appears limited to use in targeted attacks.

Source: <http://news.softpedia.com/news/Gmail-Drafts-Used-to-Exfiltrate-Data-and-Send-Malicious-Instructions-463495.shtml>

28. *October 29, Securityweek* – (International) **ICS-CERT warns of ongoing attack campaign targeting industrial control systems.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory warning about an ongoing attack campaign targeting human machine interface (HMI) products used in industrial control systems including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC products. The campaign uses a variant of the BlackEnergy malware and shares the same command and control infrastructure as the Sandworm campaign team.

Source: <http://www.securityweek.com/ics-cert-warns-ongoing-attack-campaign-targeting-industrial-control-systems>

29. *October 29, Securityweek* – (International) **Microsoft releases Fix It tool to disable SSL 3.0 in IE to muzzle Poodle attack.** Microsoft released a Fix It tool that allows users to disable SSL 3.0 in all supported versions of Internet Explorer, closing the vulnerability used in the POODLE attack. The company also announced that it will disable SSL 3.0 and fallback to SSL 3.0 by default in its products in the months ahead.

Source: <http://www.securityweek.com/microsoft-releases-fix-it-tool-disable-ssl-30-ie-muzzle-poodle-attack>

For another story, see item [33](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

30. *October 29, Detroit News* – (Michigan) **Auburn Hill man charged in cut to land line wire.** An Auburn Hills man was indicted October 28 on charges related to cutting a fiber optic wire belonging to AT&T and Comcast and disrupting phone service to as many as 600 residents, preventing them from calling emergency services.
Source: <http://www.detroitnews.com/story/news/local/oakland-county/2014/10/29/auburn-hill-man-charged-cut-land-line-wire/18104543/>

[\[Return to top\]](#)

Commercial Facilities Sector

31. *October 30, Associated Press* – (Texas) **Roof collapses at Houston-area Buddhist Center.** Authorities are investigating after a roof collapse at a prayer hall located at the Vietnamese Buddhist Center in Sugar Land October 30. No injuries were reported.
Source: http://www.brownsvilleherald.com/news/texas/article_26b27afd-a5a3-5126-aec3-920306467e37.html
32. *October 30, WWLP 22 Springfield* – (Massachusetts) **Car crashed into Deerfield restaurant; 3 hurt.** Two individuals were injured when a driver who was allegedly driving under the influence of alcohol lost control of her vehicle and crashed through the side of the Jerry's Place restaurant in Deerfield October 30. The driver also suffered minor injuries and was transported to an area hospital.
Source: <http://wwlp.com/2014/10/30/car-crashed-into-deerfield-restaurant-2-hurt/>
33. *October 30, Softpedia* – (International) **Mobile payment app contender CurrentC sees testers' details stolen.** Merchant Customer Exchange (MCX) notified adopters of CurrentC, a mobile payment app currently hosted in a trial phase, of an intrusion that revealed the email addresses of those with accounts for the testing program. The company reported that it is investigating and believes the intrusion was a result of a third-party vulnerability.
Source: <http://news.softpedia.com/news/Mobile-Payment-App-Contender-CurrentC-Sees-Testers-Details-Stolen-463568.shtml>
34. *October 29, Oakland Tribune* – (California) **Dozens become sick at NAACP annual gala in Redwood City.** More than 50 attendees of a National Association for the Advancement of Colored People (NAACP) sponsored banquet hosted at the Sofitel San Francisco Bay Hotel in Redwood were sickened by a possible foodborne illness outbreak starting October 26. Twelve individuals were transported to an area hospital while others were treated at the scene.
Source: http://www.mercurynews.com/News/ci_26818513/Dozens-become-sick-at-NAACP-annual-gala

[\[Return to top\]](#)

Dams Sector

35. *October 28, WBIR 10 Knoxville* – (Tennessee) **Chickamauga Lock closed for repairs.**

The Chickamauga Lock was shut down and traffic on the Tennessee River stalled near Chattanooga after the U.S. Army Corps of Engineers discovered an upper gate anchorage issue during a routine inspection October 27 that requires immediate repair. The closure is expected to last approximately 3 weeks.

Source: <http://www.wbir.com/story/news/local/2014/10/28/chickaumaga-lock-closed-for-repairs/18064139/>

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes .
Removal from Distribution List:	Send mail to support@govdelivery.com .

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.